(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENT- UND MARKENAMT

(12) **Offenlegungsschrift**

(10) **DE 101 00 346 A 1**

(51) Int. Cl.[7]: **H 04 L 9/22**
H 04 L 9/30
H 04 M 1/247
H 04 Q 7/32

(21) Aktenzeichen: 101 00 346.3
(22) Anmeldetag: 5. 1. 2001
(43) Offenlegungstag: 11. 7. 2002

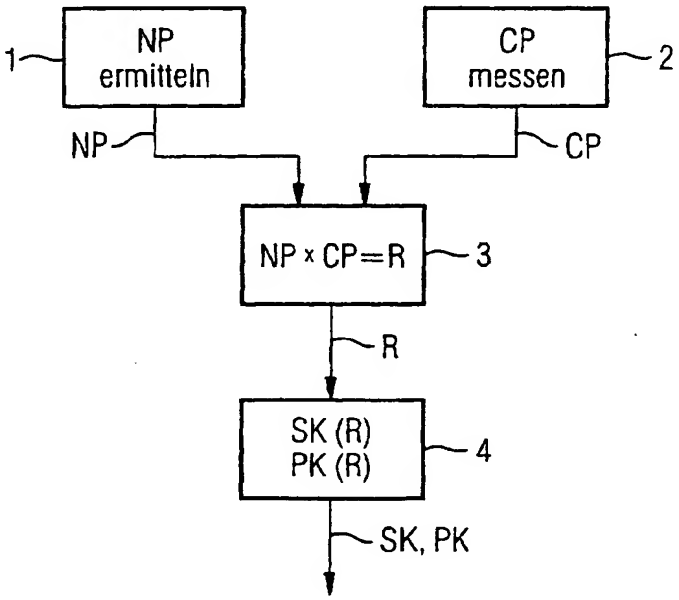
(71) Anmelder:
Siemens AG, 80333 München, DE

(72) Erfinder:
Dillinger, Markus, 81737 München, DE; Schulz, Egon, Dr., 80993 München, DE

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

(54) Verfahren zur Generierung eines Schlüssels

(57) Beschrieben wird ein Verfahren zur Generierung eines Schlüssels in einem Kommunikationsendgerät, bei dem der Schlüssel unter Verwendung eines Zufallswerts gebildet wird. Hierbei wird der Zufallswert auf Basis eines vom Kommunikationsendgerät ermittelten, zufälligen Umgebungsparameters gewonnen. Darüber hinaus wird ein entsprechendes Kommunikationsendgerät beschrieben.



DE 101 00 346 A 1

Beschreibung

[0001] Die Erfindung betrifft ein Verfahren zur Generierung eines Schlüssels in einem Kommunikationsendgerät, bei dem der Schlüssel unter Verwendung eines Zufallswerts gebildet wird. Außerdem betrifft die Erfindung ein Kommunikationsendgerät mit einer entsprechenden Einrichtung zur Generierung eines Schlüssels.

[0002] Zur Übermittlung von sicherheitsrelevanten Daten, beispielsweise beim Bezahlen per Kreditkarte oder beim Homebanking über das Internet oder auch mittels eines Mobilfunkgeräts, ist eine sichere Datenübertragung erforderlich, die zum einen eine Sicherheit gegen ein Ausspähen der Daten durch Unbefugte gewährleistet und zum anderen für den jeweiligen Empfänger die Authentizität der übermittelten Daten gewährleistet. Das heißt, es muss sichergestellt sein, dass die Daten während der Übertragung nicht in falsche Hände gelangen und missbraucht werden können, und dass die Daten nicht manipuliert wurden. Um eine solche sichere Übertragung zu gewährleisten, werden die Daten üblicherweise mit einem Schlüssel verschlüsselt und wieder entschlüsselt. Bei Verwendung eines asymmetrischen Verschlüsselungsverfahrens wird ein Schlüsselpaar – ein Schlüssel zum Ver- und ein Schlüssel zum Entschlüsseln – benötigt. Besonders sicher sind solche Verfahren dann, wenn für jede Sitzung, d. h. jede Datenverbindung, ein neuer Schlüssel bzw. ein neues Schlüsselpaar erzeugt wird, welches nur in dieser Sitzung verwendet wird (sogenannte Session Keys). Natürlich können prinzipiell die Schlüssel jederzeit vom Benutzer selbst, beispielsweise mittels einer Eingabe über eine Tastatur, frei definiert werden. Eine besonders hohe Sicherheit ist jedoch dann gegeben, wenn die Schlüssel automatisch nach einem Zufallsprinzip erzeugt werden. Hierzu kann in dem jeweiligen Kommunikationsendgerät ein Zufallsgenerator verwendet werden. Ein Nachteil solcher Zufallsgeneratoren besteht jedoch darin, dass sie in Wirklichkeit nur eine Kette von Pseudo-Zufallsfolgen produzieren. Im Übrigen müssen auch solche Zufallsgeneratoren üblicherweise zunächst durch Eingabe einer oder mehrerer (zufälliger) Zahlen initialisiert werden. Bei verschiedenen aus der Praxis bereits bekannten Homebanking-Verfahren im Internet werden die Schlüsselpaare daher durch ein zufälliges Bewegen der am Computer angeschlossenen Maus generiert. Hierzu wird der Benutzer innerhalb eines Benutzerführungsdialogs aufgefordert, mehrmals die Maus möglichst willkürlich hin- und herzubewegen. Das heißt, es ist nach wie vor eine bewusst durchgeführte Aktion des jeweiligen Benutzers erforderlich, um die Schlüssel zu erzeugen. Dieses Verfahren hat außerdem den Nachteil, dass es nur dann funktioniert, wenn das jeweilige Kommunikationsendgerät eine Maus oder ein entsprechendes Gerät, beispielsweise einen Track-Ball, aufweist. Für mobile Kommunikationsendgeräte, insbesondere Hand-held-Geräte, die in der Regel keine derartige Eingabevorrichtung aufweisen, kommt dieses Verfahren nicht in Frage.

[0003] Es ist Aufgabe der vorliegenden Erfindung, eine Alternative zu dem bekannten Stand der Technik zu schaffen, welche eine Generierung eines Schlüssels auf Basis eines zufälligen Wertes erlaubt, der ohne bewusstes Zutun eines Nutzers gefunden wurde.

[0004] Diese Aufgabe wird durch ein Verfahren gemäß Patentanspruch 1 und ein Kommunikationsendgerät gemäß Anspruch 9 gelöst.

[0005] Erfindungsgemäß wird der Zufallswert dabei auf Basis eines vom Kommunikationsendgerät ermittelten zufälligen Umgebungsparameters gewonnen. Das heißt, es werden verschiedene, am jeweiligen Kommunikationsendgerät messbare oder sonst wie ermittelbare Größen oder Charakteristiken der zufälligen Umgebung herangezogen, um den Zufallswert zu ermitteln.

[0006] Bei diesen Umgebungsparametern kann es sich um Parameter der direkten physischen Umgebung, beispielsweise Temperatur, Luftdruck, Luftfeuchtigkeit etc. handeln, die mit einer speziellen separaten Messeinrichtung des Kommunikationsendgeräts gemessen werden. Eine weitere Alternative für die Ermittlung von Umgebungswerten ist beispielsweise eine Messung der Bewegung des Geräts selbst mittels Beschleunigungsmessern im Gerät oder auch über ein GPS-System oder dergleichen.

[0007] Es kann sich aber auch um Parameter handeln, die mit dem Betrieb des Kommunikationsendgeräts zusammenhängen, beispielsweise die aktuelle Netzspannung oder Netzfrequenz, einen Akku-Ladezustand oder Ähnliches. Ebenso können auch die genaue Zeit und das Datum als Umgebungsparameter angesehen werden.

[0008] Eine spezielle Form der Umgebungsparameter sind außerdem die Kommunikationssystemparameter, d. h. solche Parameter, die die "Umgebung" des Kommunikationsendgeräts bezüglich des Kommunikationssystems beschreiben.

[0009] Hierunter fallen insbesondere Netzwerkparameter bzw. aktuelle Netzwerkeigenschaften, die z. B. davon abhängen, wo sich das Kommunikationsgerät aktuell innerhalb eines Netzwerks aufhält bzw. an welche weiteren Geräte das Kommunikationsendgerät angeschlossen ist oder mit denen es in Verbindung steht. Beispiele hierfür sind der sogenannte "BS Colorcode", ein Initialisierungscode für die vom Kommunikationsendgerät in einem Mobilfunknetz empfangenen Basisstationen, oder auch die "Sequenz Frame Numbers" der jeweiligen empfangenen Basisstation.

[0010] Eine weitere Form der Kommunikationssystemparameter sind die Kanalparameter, die die Eigenschaften des jeweils aktuell benutzten Funkkanals beschreiben. Hierunter fallen beispielsweise die aktuellen Empfangspegel(RxLEV), die BER (Bit Error Rate), die BLER (Block Error Rate), die gemessenen Interferenzen oder auch Signal-Rausch-Abstände.

[0011] Bei allen diesen Werten handelt es sich um Werte eines Mobilfunknetzes, die vom aktuellen Standort des Kommunikationsendgeräts und von den aktuellen Übertragungsbedingungen abhängen und die sich daher ständig verändern. Insbesondere bei vielen der Kommunikationssystemparameter besteht der Vorteil, dass diese Werte (wie beispielsweise die BS Colorcodes, die Sequenz Frame Numbers, die BERs und BLERs) ohnehin in regelmäßigen Abständen oder sogar permanent ermittelt bzw. gemessen werden, damit der Funkbetrieb ordnungsgemäß aufrechterhalten werden kann. Es brauchen daher nur diese bereits für andere Zwecke ermittelten Werte zur Bildung des Zufallswerts herangezogen zu werden. Eine spezielle Messung von Werten mit einer separaten Messeinrichtung, die lediglich zur Erzeugung des Zufallswerts dient, ist daher bei Verwendung dieser Parameter nicht erforderlich.

[0012] Je nach Art des Umgebungsparameters wird dieser entweder durch eine Messung ermittelt oder er wird von anderen Einrichtungen, wie beispielsweise eine Sequenz Frame Number von den jeweiligen Basisstationen, abgefragt.

[0013] Der Zufallswert kann im einfachsten Fall der ermittelte Parameter selbst sein. Ebenso kann der Zufallswert selbst im einfachsten Fall direkt als Schlüssel dienen, so dass letztlich auch der ermittelte Umgebungsparameter direkt als Schlüssel verwendet werden kann. Zur Erhöhung der Sicherheit ist es jedoch sinnvoll, wenn der Zufallswert mit einem Algorithmus aus dem ermittelten Parameter berechnet wird und ebenso mit einem weiteren Algorithmus

der Schlüssel bzw. die Schlüssel unter Verwendung des Zufallswerts ermittelt werden. Höchste Sicherheit wird erreicht, wenn die hierzu verwendeten Algorithmen geheim gehalten werden. Hierbei ist es in beliebiger Weise auch möglich, zunächst mehrere Zufallswerte zu bilden und mit Hilfe dieser verschieden Zufallswerte dann den oder die Schlüssel zu ermitteln.

[0014] Bei einem bevorzugten Ausführungsbeispiel wird der Zufallswert auf Basis einer Kombination von mehreren vom Endgerät ermittelten Umgebungsparametern gewonnen. Ein Beispiel hierfür ist die Ermittlung eines Netzwerkparameters, beispielsweise der Sequenz Frame Number der am stärksten empfangenen Basisstation, und eines Kanalparameters, beispielsweise des aktuellen Empfangspegels. Zusätzlich wird beispielsweise die genaue aktuelle Uhrzeit ermittelt und als Zufallswert wird dann das Produkt aus allen drei Werten verwendet.

[0015] Zur Erzeugung einer besonders sicheren Datenverbindung wird mit Hilfe des erfindungsgemäßen Verfahrens ein asymmetrisches Schlüsselpaar generiert. Dieses Schlüsselpaar lässt sich in beliebigen Anwendungen, beispielsweise innerhalb eines SSL (Secure Socket Layer)-Protokolls im Rahmen des sogenannten TCP/IP-Übertragungsprotokolls, verwenden.

[0016] Die Erfindung wird im Folgenden unter Hinweis auf die beigefügte Figur anhand eines Ausführungsbeispiels näher erläutert.

[0017] Die einzige Figur zeigt ein Flussdiagramm des erfindungsgemäßen Verfahrens zur Generierung eines Schlüsselpaars.

[0018] Im vorliegenden Ausführungsbeispiel wird davon ausgegangen, dass es sich um die Ermittlung eines asymmetrischen Schlüsselpaars, bestehend aus einem geheimen Schlüssel SK und einem öffentlichen Schlüssel PK handelt, die in einem Mobilfunkgerät zur Verwendung bei der Datenübertragung im Mobilfunknetz erzeugt werden. Es kann sich aber auch um ein beliebiges anderes Kommunikationsendgerät, beispielsweise ein Lap-Top, einen PC, einen Pager, oder eine PDA mit entsprechenden Kommunikationsmöglichkeiten über ein festes oder ein Mobilfunknetz oder dergleichen handeln.

[0019] Wie in der Figur zu sehen ist, wird in einem ersten Verfahrensschritt **1** ein Netzwerkparameter NP ermittelt. Hierbei handelt es sich beispielsweise um die Sequenz Frame Number der am stärksten empfangenen Basisstation. In einem weiteren Verfahrensschritt **2** wird parallel oder zeitlich versetzt ein Kanalparameter CP gemessen, beispielsweise der aktuelle Empfangspegel. In einem folgenden Verfahrensschritt **3** wird dann der Zufallswert R als Produkt aus der Sequenz Frame Number, d. h. dem Netzwerkparameter NP, und dem Empfangspegel, d. h. dem Kanalparameter CP, ermittelt.

[0020] Der so ermittelte Zufallswert R wird dann in einem weiteren Verfahrensschritt **4** einem Rechenalgorithmus zugeführt, welcher, basierend auf dem Zufallswert R, den geheimen Schlüssel SR und den öffentlichen Schlüssel PK berechnet und für die weitere Verwendung innerhalb eines Übertragungsprozesses zur Verfügung stellt. Die Schlüssel können dann in einem beliebigen enkryptischen Verfahren verwendet werden.

[0021] Ein typisches Verfahren ist hierbei das so genannte SSL-Protokoll. Bei diesem handelt es sich um ein Protokoll, welches das im Internet allgemein verwendete Übertragungsprotokoll TCP/IP um zwei weitere so genannte "Schichten" (Layer) erweitert, nämlich um das so genannte SSL-Record-Protokoll und das SSL-Handshake-Protokoll, und die Übertragung so absichert.

[0022] Unter "Layer" sind in diesem Zusammenhang die Transportschichten zu verstehen, mit denen der Datenaustausch zwischen zwei Endgeräten, beispielsweise zwei Rechnern im Internet, bildhaft dargestellt wird. Auf der obersten Ebene sind die · Anwendungen angeordnet, ganz unten befindet sich in dem Modell die Hardware. Im Idealfall lassen sich derzeit bis zu sieben Schichten definieren, denen sich wiederum im Idealfall jeweils ein Protokoll oder Programm zuordnen lässt. Alle Schichten tragen dazu bei, den Datenfluss zwischen den beiden Rechnern sicherzustellen. Das TCP/IP-Protokoll deckt daher mit seinen beiden Komponenten TCP und IP zumindest vier Schichten ab. Es wird von den meisten Betriebssystemen unterstützt. Es ist einfach zu implementieren, robust und betriebssicher, bietet jedoch keinerlei Sicherheit im Sinne einer Verschlüsselung und Authentizität der übermittelten Daten. Die Erweiterung mittels des SSL-Protokolls sorgt für diese gewünschte Sicherheit. Die beiden durch dieses Protokoll geschaffenen zusätzlichen Schichten liegen bildlich betrachtet unmittelbar aufeinander. Die Schichten sind für die angrenzenden Schichten transparent. Weder die Anwendung selbst, beispielsweise der Browser, noch die unter dem SSL-Protokoll liegenden Transportschichten des TCP/IP-Protokolls "bemerken" das Wirken des SSL-Protokolls. Daher erfordert das SSL-Protokoll weder massive Änderungen vorhandener Anwendungen noch neue Transportprotokolle.

[0023] Innerhalb des SSL-Protokolls müssen sich die beiden beteiligten Geräte, beispielsweise ein vom Nutzer verwendeter PC bzw. der dort benutzte Browser, und der Server auf einen symmetrischen Schlüssel einigen. Damit dieser Schlüssel sicher übergeben werden kann, erfolgt die Absprache in einer asymmetrischen Verschlüsselung, wozu wiederum in dem Kommunikationsendgerät des Nutzers das asymmetrische Schlüsselpaar erzeugt werden muss, was im vorliegenden Fall auf die erfindungsgemäße Weise geschehen kann.

[0024] Das Verfahren erlaubt es hierbei, auch den höchsten Sicherheitsanforderungen zur Generierung der Schlüssel gerecht zu werden, da die Schlüssel dynamisch auf rein zufällige Weise und eingabeunabhängig, d. h. ohne ein Zutun der jeweiligen Nutzer, erzeugt werden. Durch die Erfindung wird sichergestellt, dass der Schlüssel wirklich nach reinen Zufallsgrößen erzeugt wird. Eine Vorausberechnung der Schlüssel ist daher unter keinen Umständen möglich. Zudem kann das Verfahren in beliebigen Endgeräten durchgeführt werden, so dass beispielsweise das oben genannte, aus dem Internet bekannte, sichere Datenübertragungsverfahren nach dem SSL-Protokoll auch in dieser oder angepasster Form in Mobilfunknetzen angewandt werden kann.

Patentansprüche

1. Verfahren zur Generierung eines Schlüssels (SK, PK) in einem Kommunikationsendgerät, bei dem der Schlüssel (SK, PK) unter Verwendung eines Zufallswerts (R) gebildet wird, **dadurch gekennzeichnet**, dass der Zufallswert (R) auf Basis eines vom Kommunikationsendgerät ermittelten, zufälligen Umgebungsparameters (NP, CP) gewonnen wird.
2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass der Umgebungsparameter (NP, CP) einen Kommunikationssystemparameter (NP, CP) umfasst.
3. Verfahren nach Anspruch 2, dadurch gekennzeichnet, dass der Kommunikationssystemparameter (NP) einen Netzwerkparameter (NP) umfasst.
4. Verfahren nach Anspruch 2 oder 3, dadurch gekennzeichnet, dass der Kommunikationssystemparameter (CP) einen Kanalparameter (CP) umfasst.
5. Verfahren nach einem der Ansprüche 1 bis 4, da-

durch gekennzeichnet, dass der Zufallswert (R) auf Basis einer Kombination von mehreren vom Endgerät ermittelten Umgebungsparametern (NP, CP) gewonnen wird.

6. Verfahren nach einem der Ansprüche 1 bis 5, dadurch gekennzeichnet, dass der Schlüssel (SK, PK) innerhalb eines SSL-Protokolls zur Sicherung einer Datenübertragung verwendet wird.

7. Verfahren nach einem der Ansprüche 1 bis 6, da durch gekennzeichnet, dass ein Schlüsselpaar (SK, PK) generiert wird.

8. Verfahren nach einem der Ansprüche 1 bis 7, dadurch gekennzeichnet, dass zur Bildung des Schlüssels (SK, PK) ein Umgebungsparameter (NP, CP) verwendet wird, der zum Betrieb des Kommunikationsendgeräts in einer bestimmten Betriebsfunktion permanent oder in zeitlichen Abständen wiederholt ermittelt wird.

9. Kommunikationsendgerät mit einer Einrichtung zur Generierung eines Schlüssels (SK, PK) unter Verwendung eines Zufallswerts (R), dadurch gekennzeichnet, dass das Kommunikationsendgerät eine Einrichtung zum Ermitteln eines zufälligen Umgebungsparameters (NP, CP) aufweist und die Einrichtung zur Generierung des Schlüssels (SK, PK) derart aufgebaut ist, dass der Schlüssel (SK, PK) unter Verwendung eines Zufallswerts (R) gebildet wird, der auf Basis des ermittelten Umgebungsparameters (NP, CP) gewonnen wird.

10. Kommunikationsendgerät nach Anspruch 9, dadurch gekennzeichnet, dass die Einrichtung zur Generierung des Schlüssels Mittel zur Übernahme eines Umgebungsparameters aufweist, der zum Betrieb des Geräts in einer bestimmten Betriebsfunktion permanent oder in zeitlichen Abständen wiederholt ermittelt wird.

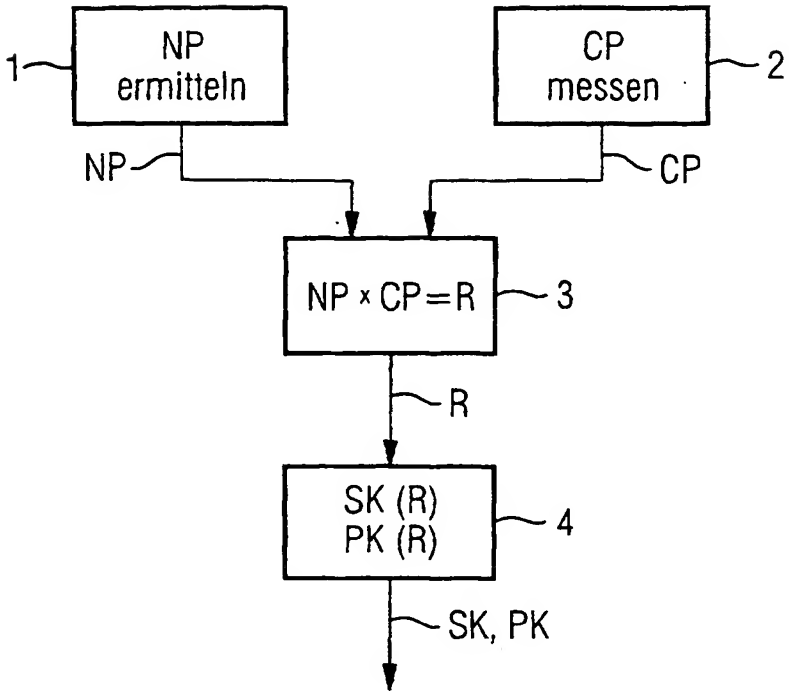
11. Kommunikationsendgerät nach Anspruch 9 oder 10, gekennzeichnet durch eine separate Messeinrichtung zum Messen eines Umgebungsparameters für die Einrichtung zur Generierung des Schlüssels.

12. Kommunikationsendgerät nach einem der Ansprüche 9 bis 11, dadurch gekennzeichnet, dass das Kommunikationsendgerät ein mobiles Kommunikationsendgerät ist.

Hierzu 1 Seite(n) Zeichnungen

- Leerseite -

Nummer: DE 101 00 346 A1
Int. Cl.[7]: H 04 L 9/22
Offenlegungstag: 11. Juli 2002



Verfahren zur Generierung eines Schlüssels

Publication number: DE10100346
Publication date: 2002-07-11
Inventor: DILLINGER MARKUS (DE); SCHULZ EGON (DE)
Applicant: SIEMENS AG (DE)
Classification:
- international: ***H04L9/30; H04L29/06; H04Q7/32;*** **H04L9/28; H04L29/06; H04Q7/32;** (IPC1-7): H04L9/22; H04L9/30; H04M1/247; H04Q7/32
- european: H04Q7/32S; H04L9/30; H04L29/06C6B
Application number: DE20011000346 20010105
Priority number(s): DE20011000346 20010105

Also published as:
WO02054807 (A

Abstract of **DE10100346**

The invention relates to a method for generating a key in a communication terminal, according to which the key is generated using a random value. Said random value is acquired on the basis of a random environment parameter acquired by the communication terminal. The invention further relates to a corresponding communication terminal. Said communication terminal is preferably a mobile communication device in which network and/or channel parameters are acquired as environment parameters. Preferably, the secure socket layer protocol (SSL) is used in a TCP/IP protocol. The communication device is preferably a lap top PC, a pager or a personal digital assistant (PDA) connecte to a mobile radio network.

This Page Blank (uspto)

Docket # 2004P00922
Applic. #
Applicant: Franke, et al.
Lerner Greenberg Stemer LLP
Post Office Box 2480
Hollywood, FL 33022-2480
Tel: (954) 925-1100 Fax: (954) 925-1101